What is claimed is:

1. A symmetric-key encryption method comprising the steps of:

dividing plaintext composed of redundancy data and a message to generate a plurality of plaintext blocks each having a predetermined length;

generating a random number sequence based on a secret key;

generating a random number block corresponding to one of said plurality of plaintext blocks from said random number sequence;

outputting a feedback value obtained as a result of operation on said one of the plurality of plaintext blocks and said random number block, said feedback value being fed back to another one of the plurality of plaintext blocks; and

performing an encryption operation using said one of the plurality of plaintext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of plaintext blocks to produce a ciphertext block.

2. The symmetric-key encryption method as claimed in claim 1, wherein said encryption operation uses one or more said random number blocks whose total length is longer than

a length of said ciphertext block.

3. The symmetric-key encryption method as claimed in claim 2, wherein said plaintext further includes secret data of a predetermined length.

4. The symmetric-key encryption method as claimed in claim 2, wherein said encryption operation performs a binomial operation or a monomial operation using one of said plurality of plaintext blocks one or more times according to a predetermined procedure, combines a plurality of obtained ciphertext blocks, and outputs the combined plurality of ciphertext blocks as ciphertext.

5. The symmetric-key encryption method as claimed in claim 2, wherein said encryption operation includes multiplication and addition in a finite field.

6. The symmetric-key encryption method as claimed in claim 2, wherein said encryption operation includes a combination of a cyclic shift operation and arithmetic multiplication.

7. The symmetric-key encryption method as claimed in claim 2, wherein said symmetric-key encryption method employs a pseudorandom-number generating means for generating said random number sequence based on said secret key.

8. The symmetric-key encryption method as claimed in claim 7, further comprising steps of:

dividing said message into a plurality of message blocks;

generating a number of random number sequences equal to the number of said plurality of message blocks using said pseudorandom-number generating means; and

performing parallel processing by assigning said plurality of message blocks to one operation unit and assigning said number of random number sequences to another operation unit.

9. A symmetric-key decryption method comprising the steps of:

dividing ciphertext to generate a plurality of ciphertext blocks each having a predetermined length;

generating a random number sequence based on a secret key;

generating a random number block corresponding to one of said plurality of ciphertext blocks from said random number sequence;

outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back to another one of the plurality of ciphertext blocks; and

performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block.

10. The symmetric-key decryption method as claimed in claim 9, wherein said decryption operation uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks.

11. The symmetric-key decryption method as claimed in claim 10, further comprising steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

12. The symmetric-key decryption method as claimed in claim 11, further comprising steps of:

extracting secret data included in said plaintext; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

13. A symmetric-key encryption apparatus comprising:

a circuit for receiving plaintext composed of redundancy data and a message, and dividing the received plaintext to generate a plurality of plaintext blocks each having a predetermined length;

a circuit for receiving a secret key to generate a random number sequence, and generating a random number block corresponding to one of said plurality of plaintext blocks from said random number sequence;

a circuit for outputting a feedback value obtained as a result of operation on said one of the plurality of plaintext blocks and said random number block, said feedback value being fed back to another one of the plurality of plaintext blocks; and

an encryption operation circuit for performing an encryption operation using said one of the plurality of plaintext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of plaintext blocks and another random number block to produce a ciphertext block.

14. The symmetric-key encryption apparatus as claimed in claim 13, wherein said encryption operation circuit uses one or more said random number blocks whose total length is longer than a length of said ciphertext block.

15. The symmetric-key encryption apparatus as claimed in claim 14, wherein said plaintext further includes secret data of a predetermined length.

16. The symmetric-key encryption apparatus as claimed in claim 14, wherein said encryption operation circuit includes:

a circuit for performing a binomial operation or a monomial operation using one of said plurality of plaintext blocks one or more times according to a predetermined procedure; and

a circuit for combining a plurality of obtained ciphertext blocks, and outputting the combined plurality of ciphertext blocks as ciphertext.

17. The symmetric-key encryption apparatus as claimed in claim 14, wherein said encryption operation circuit performs multiplication and addition in a finite field.

18. The symmetric-key encryption apparatus as claimed in claim 14, wherein said encryption operation circuit includes a cyclic shift operation circuit and an arithmetic multiplication circuit.

19. The symmetric-key encryption apparatus as claimed in claim 14, further comprising:

a pseudorandom number generator for generating said random number sequence based on said secret key.

20. The symmetric-key encryption apparatus as claimed in claim 19, further comprising:

a circuit for dividing said message into a plurality of message blocks;

a circuit for generating a number of random number sequences equal to the number of said plurality of message blocks using said pseudorandom number generator;

a plurality of operation units; and

a circuit for assigning said plurality of message blocks to one of the plurality of operation units and assigning said number of random number sequences to another one of the plurality of operation units.

21. A symmetric-key decryption apparatus comprising:

a circuit for receiving ciphertext, and dividing the received ciphertext to generate a plurality of ciphertext blocks each having a predetermined length;

a circuit for receiving a secret key to generate a random number sequence whose length is longer than a length of said ciphertext, and generating a random number block corresponding to one of said plurality of ciphertext blocks from said random number sequence;

a circuit for outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back to another one of the plurality of ciphertext blocks; and

a decryption operation circuit for performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block.

22. The symmetric-key decryption apparatus as claimed in claim 21, wherein said decryption operation circuit uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks.

23. The symmetric-key decryption apparatus as claimed in claim 22, further comprising:

a circuit for concatenating a plurality of said plaintext blocks to generate plaintext;

a circuit for extracting redundancy data included in said plaintext; and

a circuit for checking said redundancy data to detect whether said ciphertext has been altered.

24. The symmetric-key decryption apparatus as claimed in claim 23, further comprising:

a circuit for extracting secret data included in said plaintext,

wherein said circuit for detecting whether said ciphertext has been altered checks said secret data and said redundancy data to detect whether said ciphertext has been altered.

25. A medium storing a program for causing a computer to perform a symmetric-key encryption method, wherein said program is read into said computer, said symmetric-key encryption method comprising the steps of:

reading plaintext composed of redundancy data and a message, and dividing said plaintext to generate a plurality of plaintext blocks each having a predetermined length;

receiving a secret key to generate a random number sequence, and generating a random number block corresponding to one of said plurality of plaintext blocks from said random number sequence;

outputting a feedback value obtained as a result of operation on said one of the plurality of plaintext blocks and said random number block, said feedback value being fed back to another one of the plurality of plaintext blocks; and

performing an encryption operation using said one of the plurality of plaintext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of plaintext blocks and another random number block to produce a ciphertext block.

26. The medium storing a program as claimed in claim 25, wherein said encryption operation uses one or more said random number block whose total length is longer than a

length of said ciphertext block.

27. The medium storing a program as claimed in claim 26, wherein said plaintext further includes secret data of a predetermined length.

28. The medium storing a program as claimed in claim 26, wherein said encryption operation performs a binomial operation or a monomial operation using one of said plurality of plaintext blocks one or more times according to a predetermined procedure, combines a plurality of obtained ciphertext blocks, and outputs the combined plurality of ciphertext blocks as ciphertext.

29. The medium storing a program as claimed in claim 26, wherein said encryption operation includes multiplication and addition in a finite field.

30. The medium storing a program as claimed in claim 26, wherein said encryption operation includes a cyclic shift operation and arithmetic multiplication.

31. The medium storing a program as claimed in claim 26, wherein said symmetric-key encryption method further comprises a step of:

generating pseudorandom numbers to generate said random number sequence based on said secret key.

32. The medium storing a program as claimed in claim 31, wherein said symmetric-key encryption method further comprises steps of:

dividing said message into a plurality of message blocks;

generating said pseudorandom numbers so as to generate a number of random number sequences equal to the number of said plurality of message blocks; and

assigning said plurality of message blocks to one operation unit and assigning said number of random number sequences to another operation unit.

33. A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said symmetric-key decryption method comprising the steps of:

receiving ciphertext, and dividing the received ciphertext to generate a plurality of ciphertext blocks each having a predetermined length;

receiving a secret key to generate a random number sequence whose length is longer than a length of said ciphertext, and generating a random number block corresponding to one of said plurality of ciphertext blocks from said random number sequence;

outputting a feedback value obtained as a result of operation on said one of the plurality of ciphertext blocks and said random number block, said feedback value being fed back to another one of the plurality of ciphertext blocks; and performing a decryption operation using said one of the plurality of ciphertext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of ciphertext blocks to produce a plaintext block.

34. The medium storing a program as claimed in claim 33, wherein said decryption operation uses one or more said random number blocks whose total length is longer than a length of said one of the plurality of ciphertext blocks.

35. The medium storing a program as claimed in claim 34, wherein said symmetric-key decryption method further comprises steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

36. The medium storing a program as claimed in claim 35, wherein said symmetric-key decryption method further comprises steps of:

extracting secret data included in said plaintext; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

37. A program product for causing a computer to perform a symmetric-key encryption method, wherein said program product is read into said computer, said program product comprising:

code for causing said computer to read plaintext composed of redundancy data and a message, and divide said plaintext to generate a plurality of plaintext blocks each having a predetermined length;

code for causing said computer to receive a secret key to generate a random number sequence, and generate a random number block corresponding to one of said plurality of plaintext blocks from said random number sequence;

code for causing said computer to output a feedback value obtained as a result of operation on said one of the plurality of plaintext blocks and said random number block, said feedback value being fed back to another one of the plurality of plaintext blocks; and

code for causing said computer to perform an encryption operation using said one of the plurality of plaintext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of plaintext blocks and another random number block to produce a ciphertext block,

wherein said program product is stored in a medium readable by said computer for embodying said codes.